Please amend the claims as follows:

1. (Currently Amended) Method for decrypting data within a playback device, the data comprising an encrypted first data set being audio-visual presentation data and an encrypted second data set being audio-visual supplementary data relating to the first data set, wherein said first data set and at least two ~~respective~~ corresponding device independent electronic decryption ~~key~~ keys are stored on a first removable prerecorded storage medium, and the second data set is not stored on the first removable prerecorded storage medium but on a second ~~data source~~ storage medium within said playback device and is related to the first data set, the second ~~data source~~ storage medium having a first data block that is public, a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the first removable prerecorded storage medium, the method comprising the steps of
   - retrieving the first data set and the device independent decryption keys from the first removable storage medium;
   - retrieving the second data set from the second data block of the second ~~data source~~ storage medium;
   - decrypting the first data set using a first of said decryption keys; and
   - decrypting the second data set using a second of said decryption keys that ~~are~~ is different from the first of said decryption keys.

2. (Currently amended) Method according to claim 1, further comprising the step of determining from a plurality of data sets on the second ~~data source~~ storage medium a second data set that refers to the first removable storage medium, wherein the data sets refer to different removable prerecorded storage media.

3. (Currently amended) Method according to claim 1, further comprising the step of detecting whether the first removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as

authorized if it can be decrypted by said second decryption key.

4. (Previously Presented) Method according to claim 1, wherein the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains said electronic decryption keys is readable.

Claims 5-17: (Cancelled)

18. (New) Apparatus for decrypting data within a playback device, the data comprising an encrypted first data set being audio-visual presentation data and an encrypted second data set being audio-visual supplementary data relating to the first data set, wherein said first data set and at least two corresponding device independent electronic decryption keys are stored on a first removable prerecorded storage medium, and the second data set is not stored on the first removable prerecorded storage medium but on a second storage medium within said playback device and is related to the first data set, the second storage medium having a first data block that is public, a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the first removable prerecorded storage medium, the apparatus comprising

- means for retrieving the first data set and the device independent decryption keys from the first removable storage medium;
- means for retrieving the second data set from the second data block of the second storage medium;
- means for decrypting said first data set using a first of said decryption keys; and
- means for decrypting said second data set using a second of said decryption keys, the second decryption key being different from said first decryption key.

19. (New) Apparatus according to claim 18, further comprising means for determining from a plurality of data sets on the second storage medium a second data set that refers to the first removable storage medium, wherein the data sets refer to different

removable prerecorded storage media.

20. (New) Method according to claim 1, wherein the first electronic decryption key is the only suitable key for decrypting the first data set, and the second decryption key is one of several suitable keys for decrypting the second data set.

21. (New) Method according to claim 1, wherein the first and second data sets are encrypted using RSA (Rivest-Shamir-Adelman) coding.

22. (New) Apparatus according to claim 18, further comprising means for detecting whether the first removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as authorized if it can be decrypted by said second decryption key.

23. (New) Apparatus according to claim 18, wherein the first electronic decryption key is the only suitable key for decrypting the first data set, and the second electronic decryption key is one of several suitable keys for decrypting the second data set.

24. (New) Apparatus according to claim 18, wherein only encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered.

25. (New) Apparatus according to claim 18, wherein the specified group of removable storage media comprises only media that are provided by a particular provider.

26. (New) Method according to claim 1, further comprising the steps of retrieving a third data set from the third data block, and decrypting the third data set using the second of the decryption keys.

27. (New) Method according to claim 1, wherein only encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered.

28. (New) Method according to claim 1, wherein the specified group of removable storage media comprises only media that are provided by a particular provider.

29. (New) Method according to claim 1, wherein the second data block of said second data set can only be decrypted if any one of said specified group of removable storage media is accessible.

30. (New) Method according to claim 29, wherein said specified group of removable storage media is a pre-defined group that is provided by the same provider as said first removable storage medium.

31. (New) Apparatus according to claim 18, wherein the second data block of said second data set can only be decrypted if any one of said specified group of removable storage media is accessible.

32. (New) Apparatus according to claim 31, wherein said specified group of removable storage media is a pre-defined group that is provided by the same provider as said first removable storage medium.